



i n v e n t



Cyber-Investigation on Cyber-Crime

Ricci Leong and Vincent Ip,
Security Consultant,

HP e-Security Center, HP
Consulting, HK

E-Commerce leads to Cyber Crime

- US\$30 billion in 2001 in Internet commerce revenue in 16 Western European countries (ZDNet March 9, 1998)
- US\$1.3 trillion by 2003 in Internet Business transaction (Forrester Research)
- Number of Unique Visitors increased in most of the B2C web sites by around 50% (CyberAtlas.internet.com, 8 Jan 2001)
- B2C Internet Commerce Market in 2001 will be US\$95 billion (IDC, 4 Jan 2001)

How secure are you?

- Internet connection?
- Firewall protection?
- Intrusion Detection System installed?
- Frequently reviewed of security logs? (including firewall logs, router logs, mail server logs, web server logs, etc)
- Encryption of email message?
- Security Risk Assessment performed periodically?
- 24x7 security monitoring?

More potential target for
hackers

By May 2001

Apache 62.24%

Microsoft IIS 20.52%

iPlanet 6.13%

Zeus 2.75%

Rapidsite 1.40%

AOLserver 1.30%

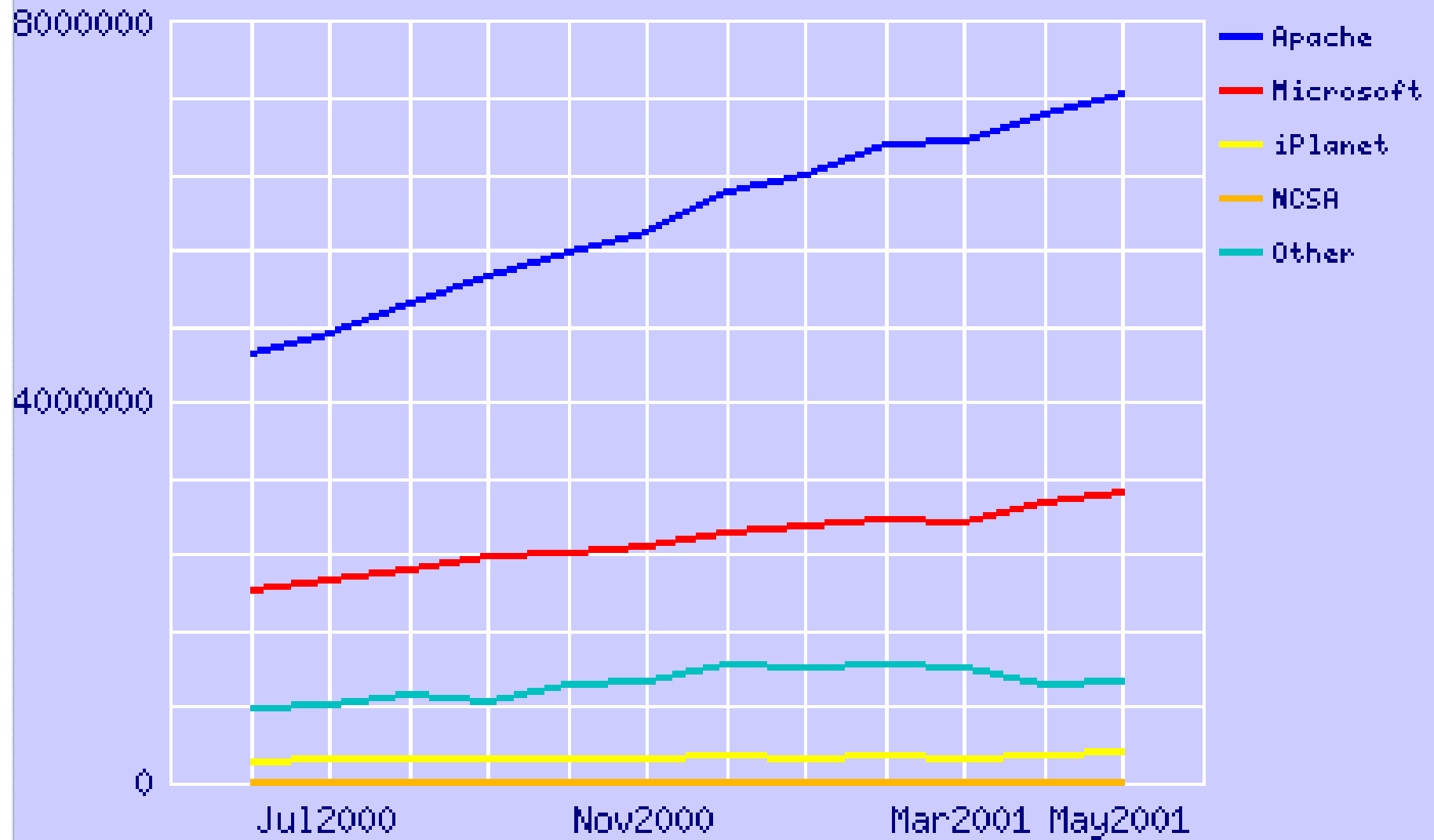
Thttpd 1.28%

Tigershark 0.74%

WebSitePro 0.41%

ConcentricHost-Ashurbanipal
0.38%

Active Servers – Potential target list



Statistics on Web defacement (from Attrition.org)

alldas.de defacement archives - Microsoft Internet Explorer provided by HutchHome

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit

Address <http://defaced.alldas.de/defaced.php?archives=os> Go

Links Channel Guide Customize Links Free HotMail Internet Start Microsoft RealPlayer Windows Update Windows Klink

Misc:News - Library - Disclaimer - Administrator-FAQ - Defacer-FAQ - The Staff

defacements search engine

search defaced site

Join Alldas.de Defaced Archives MailingLists!

Your E-Mail Address

Subscribe

latest news of alldas

We've decided to stay with our ISP

New section: Library

Alldas.de Defacement Mirror temporary Offline

> OS Statistics for 18892 defaced Websites.

> 17 different OS's since 04/2000

12226 times	a " Windows "	Host has been defaced, which is 64.72percent of all archived defacements
3358 times	a " Linux "	Host has been defaced, which is 17.77percent of all archived defacements
1967 times	a " Unknown "	Host has been defaced, which is 10.41percent of all archived defacements
593 times	a " Solaris "	Host has been defaced, which is 3.14percent of all archived defacements
278 times	a " IRIX "	Host has been defaced, which is 1.47percent of all archived defacements
182 times	a " FreeBSD "	Host has been defaced, which is 0.96percent of all archived defacements
145 times	a " BSDI "	Host has been defaced, which is 0.77percent of all archived defacements
72 times	a " SCO "	Host has been defaced, which is 0.38percent of all archived defacements
23 times	a " NetBSD "	Host has been defaced, which is 0.12percent of all archived defacements
11 times	a " AIX "	Host has been defaced, which is 0.06percent of all archived defacements
9 times	a " HP-UX "	Host has been defaced, which is 0.05percent of all archived defacements
8 times	a " Tru64 UNIX "	Host has been defaced, which is 0.04percent of all archived defacements
7 times	a " Digital Unix "	Host has been defaced, which is 0.04percent of all archived defacements
6 times	a " MacOs "	Host has been defaced, which is 0.03percent of all archived defacements
5 times	a " OpenBSD "	Host has been defaced, which is 0.03percent of all archived defacements
1 time	a " Novell "	Host has been defaced, which is 0.01percent of all archived defacements
1 time	a " Ultrix "	Host has been defaced, which is 0.01percent of all archived defacements

Internet 2 Free Air Tickets

Increase in Crime number

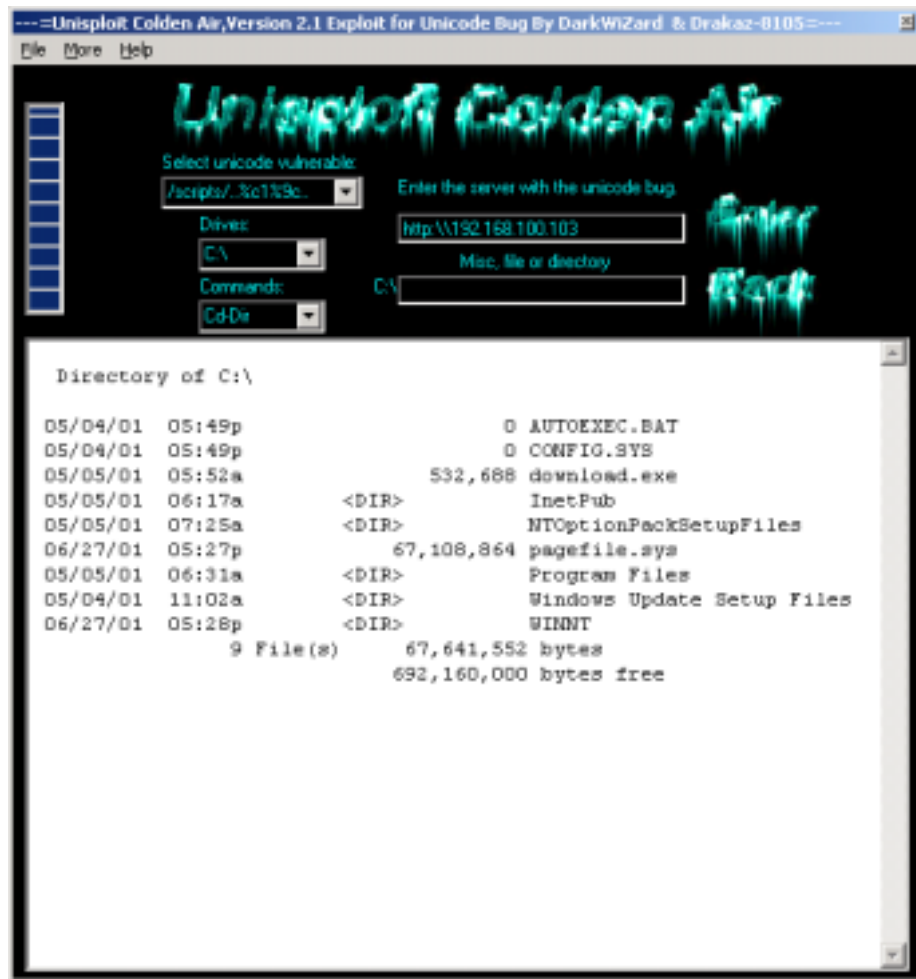
2001 CSI/FBI Computer Crime and Security Survey

- 538 responses
- 64% of respondents detected “unauthorized use of computer systems” in the last 12 months
- 40% detected “system penetration”
 - 95% had 1 firewall
 - 61% had an IDS
- 26% detected “theft of proprietary info”
- 18% detected “sabotage”
- Combined losses from 196 respondents totaled \$378 million
 - \$151 million from “theft of proprietary info”
 - \$19 million from “system penetration”

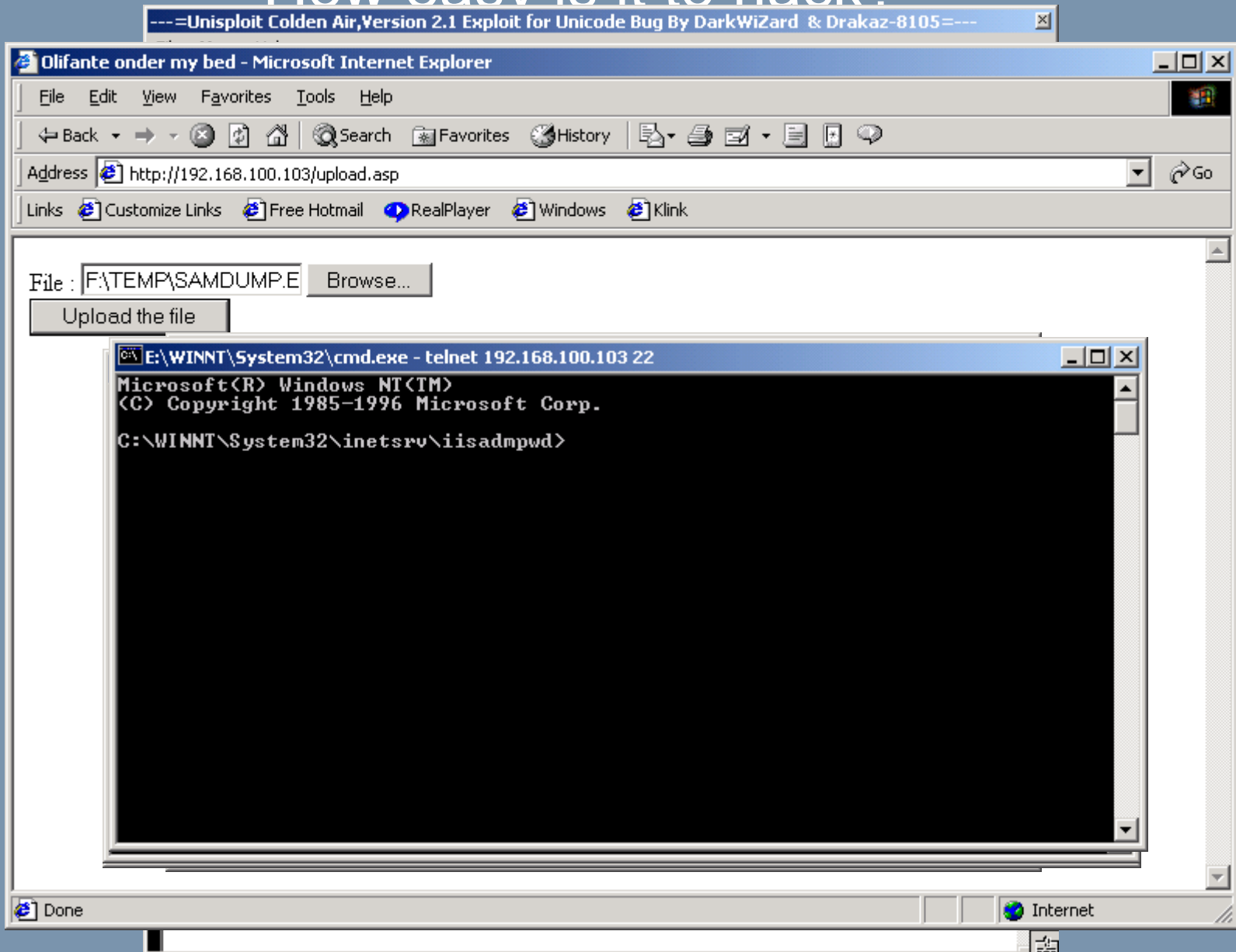
Targeted platform

- Hackers crack four Microsoft sites (22/6/2001)
- Oracle Security Risk On Windows NT (26/6/2001)
 - “This vulnerability causes a Windows NT system to consume 100% of available memory. Access to the server is denied and a full reboot is required”
- Solaris Bug Gives Attackers System-Level Access (21/6/2001)
 - “A newly discovered bug in Solaris could allow attackers to run malicious programs on servers with Sun's operating system installed”
- Apache.org got defaced (30/5/2001)

Hacking is as easy as
click a button



How easy is it to hack?



Vulnerabilities are always with you

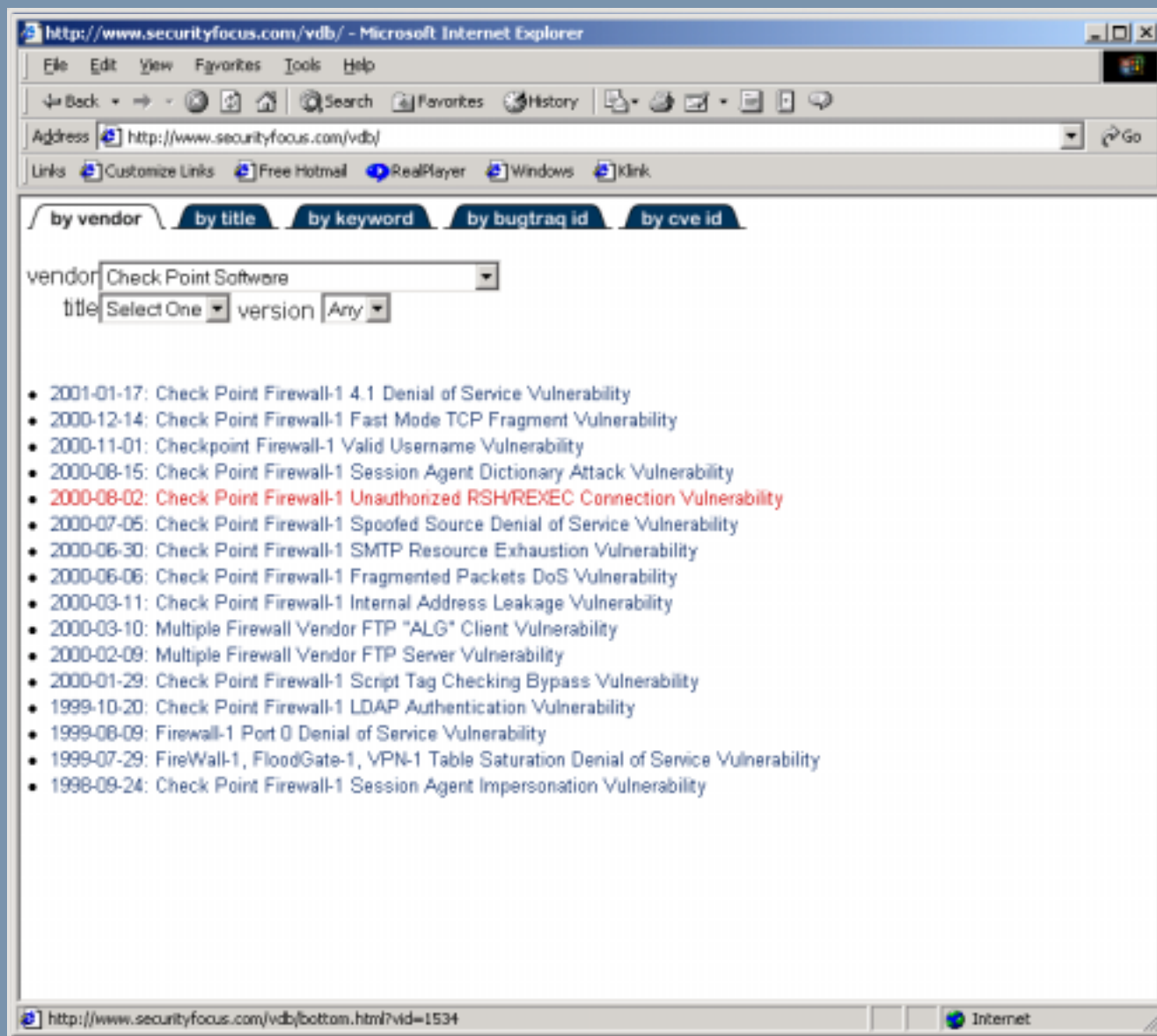
Adobe Acrobat - [cyberissue2001-12.pdf]

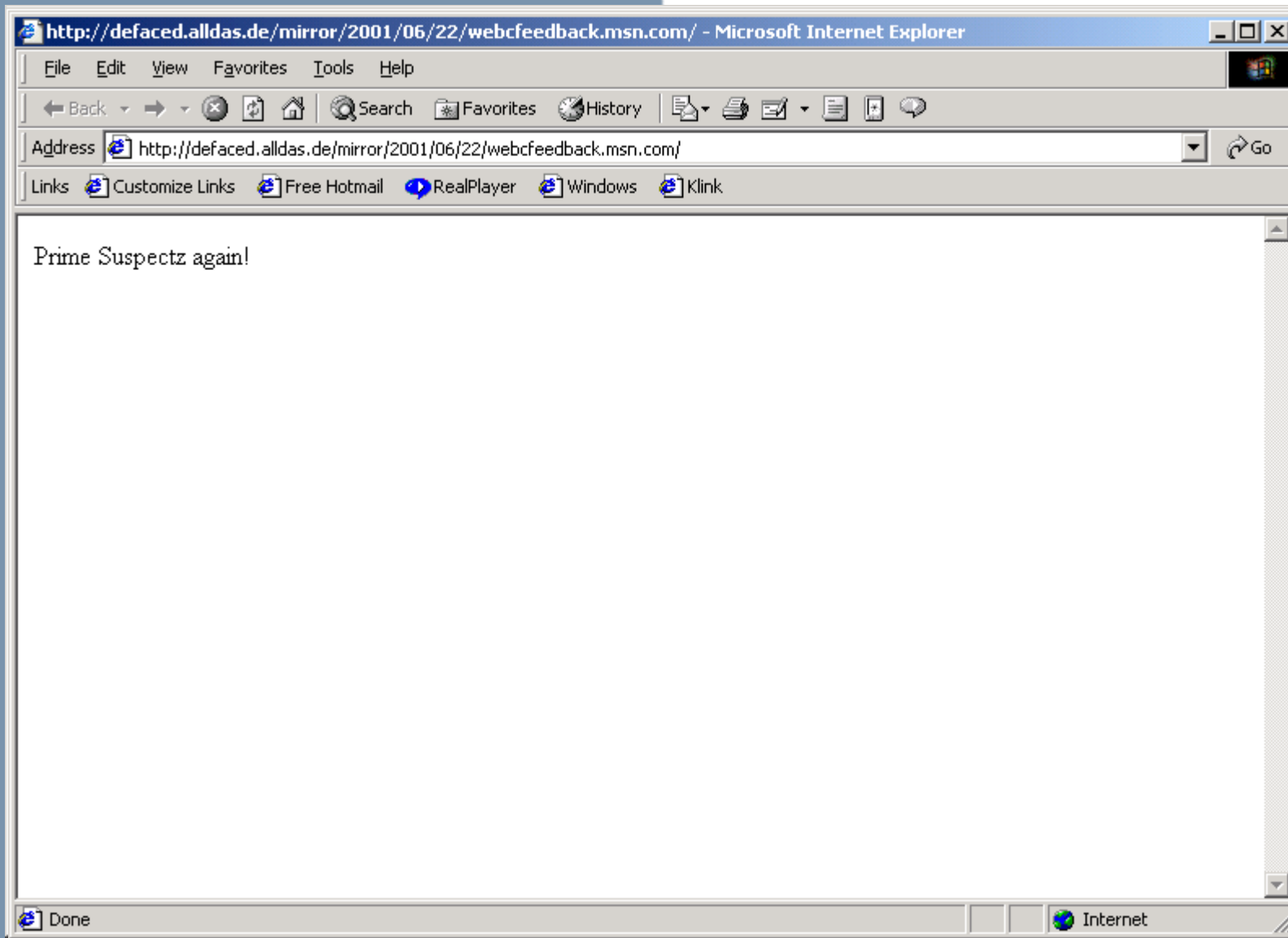
File Edit Document Tools View Window Help

	NT 4.0/2000		using a fixed master key, which could let a malicious user break the algorithm and gain access to all login information.	password encryption.	password Encryption		and websites.
PKCrew™	Unix	TIA Tunnel 0.9alpha2, 0.9alpha3	A buffer overflow vulnerability exists in the authentication mechanism, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://tatunnel.pkcres.org/download/tatunnel-0.9alpha3.tar.gz	TIA Tunnel Authentication Mechanism Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Pragma Systems™	Windows 95/98/NT 4.0	InterAccess TelnetD Server 4.0, 4.0 Build 4 & 5	A Denial of Service vulnerability exists if large bursts of data are sent to port 23 (Telnet).	Upgrade available at: http://www.pragmasys.com/Downloads.html	InterAccess Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Qualcomm	Multiple	qpopper 4.0-4.0.2	A buffer overflow vulnerability exists in the qpopper source tree, which could let a remote malicious user gain root privileges.	Upgrade available at: http://ftp.qualcomm.com/reader/aservers/isis/qpopper/qpopper4.0.3.tar.gz	qpopper Username Buffer Overflow	High	Bug discussed in newsgroups and websites.
RedHat™	Unix	Linux 6.1, 6.2, 7.0, 7.1	A buffer overflow vulnerability exists in the implementation of the 'man' system manual pager program, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Linux Man Page Source Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
RedHat™	Unix	Linux 7.0 alpha, i386, 7.1 i386	A vulnerability exists in the xinetd daemon, which could let a malicious user create world-writable files.	Upgrade available at: http://updates.redhat.com/	Xinetd Insecure Default Umask	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat™	Unix	Ken Stevens ispell 3.1.20	A vulnerability exists in versions of ispell due to the way gnomerpm handles tmp files, which could let a malicious user create or overwrite files.	Upgrade available at: http://updates.redhat.com/	Ken Stevens ispell Symbolic Link	Medium	Bug discussed in newsgroups and websites.
SCO™	Unix	Unixware 7.0- 7.1.1	A buffer overflow vulnerability exists in the implementation of libtermcap used by Unixware, which could let a malicious user elevate their privileges.	No patch or patch available at time of publishing.	Unixware Libtermcap Buffer Overflow	Medium	Bug discussed in newsgroups and websites.

125% 8 of 20 8.5 x 11 in

Vulnerabilities are always with you





netpu
hacke

Can we identify the attack?

This is the simplest case in investigation

- From viewing the web directly
- From defacement mailing list
- By external web user

What to do next

Immediate work

- Incident Handling
 - should be meeting the requirements from legal counsel, business, law enforcement and company managers

Afterwards

- Computer Crime and Forensics Investigation
 - usually performed by the 3rd party company, CERT or law enforcement team

Managed Security Services

- On-site Consulting
- Outsource Security Management
 - Remote perimeter management
 - 24x7 Management and monitoring services
- Penetration and vulnerability testing
- Incident Handling and Computer Forensics Investigation
 - Incident Handling
 - **Computer Forensics Investigation**

How to perform Computer Forensics Investigation?

Identify the Incident,
then the Evidence

Collect and Preserve the
Evidence

Investigation:
Extract, process, and
interpret

Step 1 - Incident Identification

- Initial Response by the system administrator
 - retrieve information to confirm the incident
 - review from all possible sources of the information
 - identify the scope and size of the affected machines and systems
 - determine the damage caused by the intrusion (if any)
 - identify the possible path of attack
 - Backup all possible evidence

Step 1 - Incident Identification

- Important notes
 - try to prevent modification of the original
 - keep the chain of custody
 - make at least two copies
 - sign and confirm the date of the original
 - check the system clock and time on affected machines

Our Forensics Toolbox

- Traveling forensics lab
 - Boot disks
 - Backup hard disk devices
 - Sniffer machines
 - man pages and manual of different platform
 - Tools for *nix
 - dd, netcat, TCT, TCTUtil, ls, ps, lsof, md5sum, find, netstat, ifconfig, strings, trace, who, w, last, lastlog, tcpdump, unrm, lazarus etc
 - Tools for Windows
 - cmd.exe, date, time, loggedon, IRCR, fport, netstat, listdlls, doskey, uptime, nbtstat, pslist, auditpol, afind, ntlast, dumpel, regdump, pwdump, windump, md5sum, userinfo, sig, getslack, inzider etc

Step 2 - Evidence Collection

Preserving the evidence in Hard disk

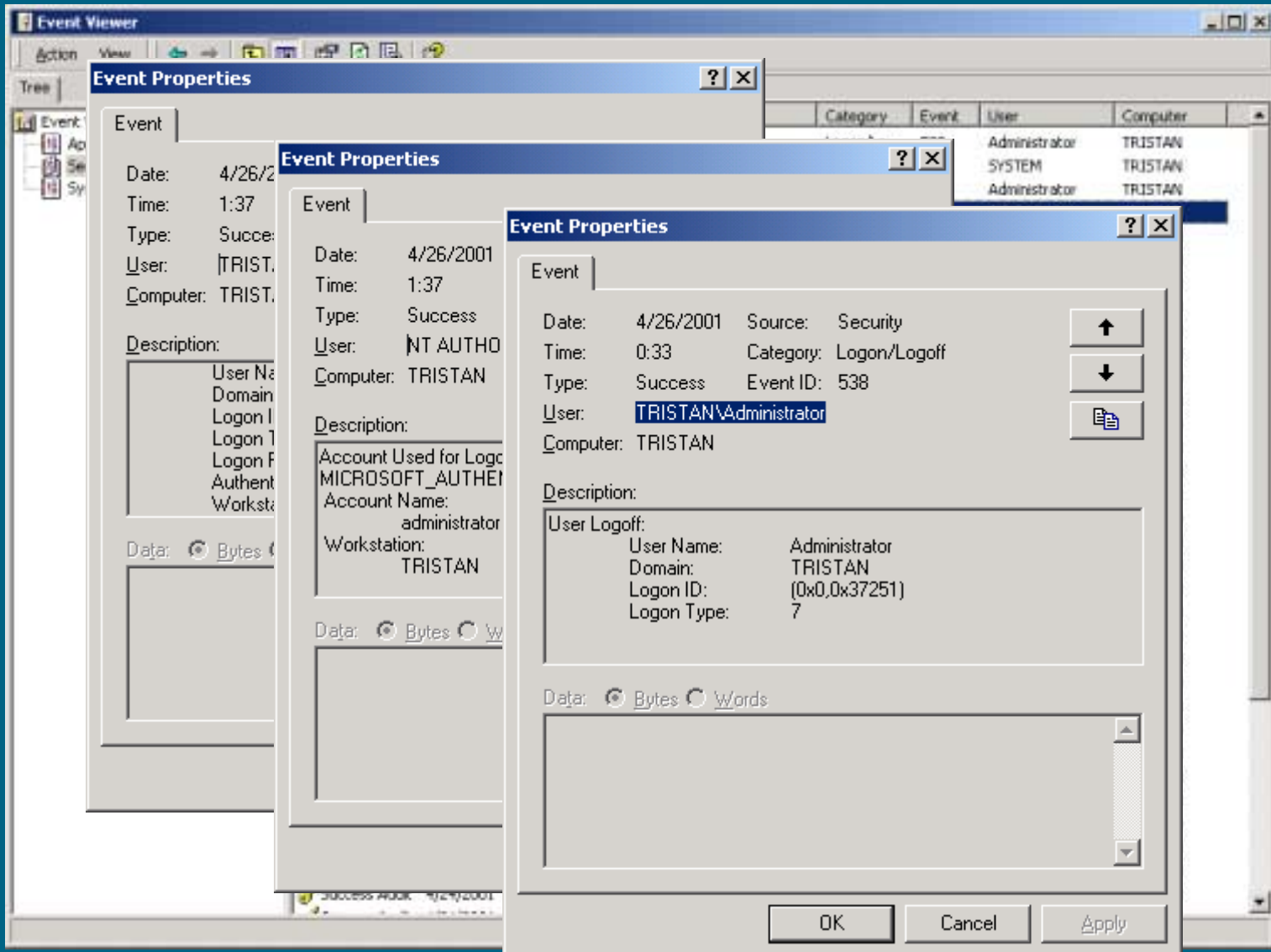
- Cloning of disk based on
 - dd and md5
 - Encase
 - SafeBack
 - Ghost
 - Disk Duplicator
- Near to Exact Copy
 - Back up from backup tape

Step 2 - Evidence Collection

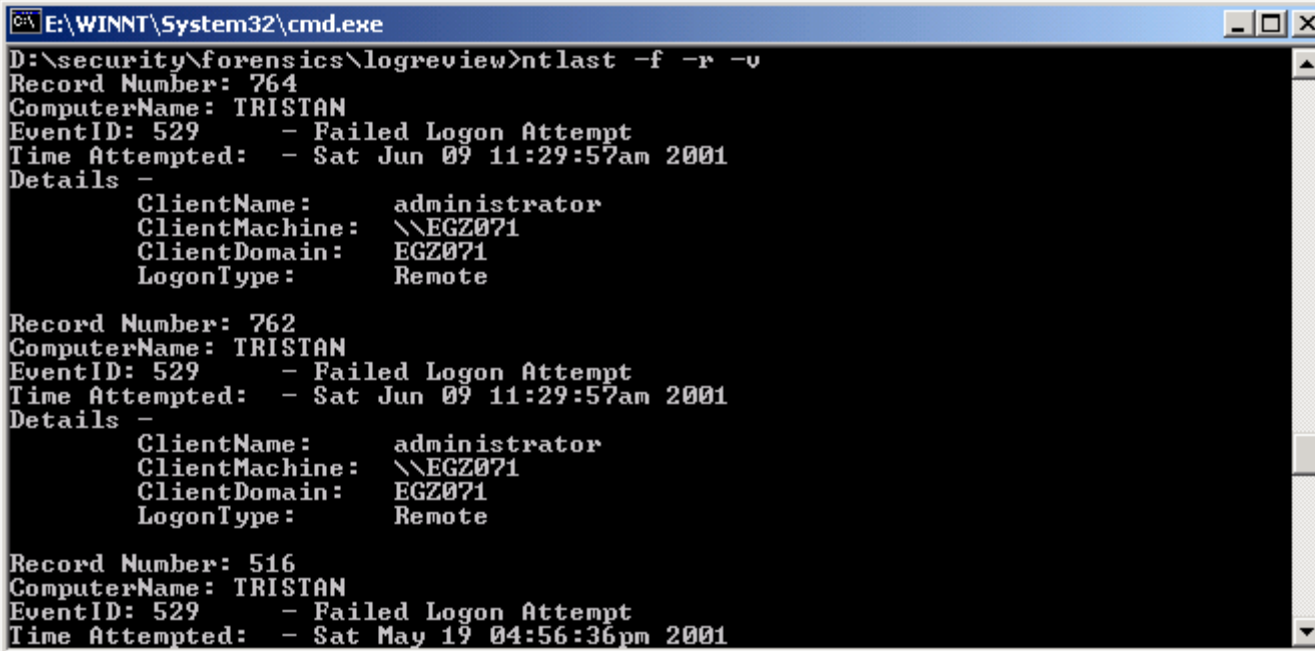
Collect the state of the machine

- Network information
 - netstat, ipconfig, nbtstat, etc.
- Process information
 - ps, pslist, etc
- Open ports and hidden services
 - lsof, fport, inzider, etc
- Log files
 - Phone log, Web server log, mail server log, ftp log, router log, firewall log
 - who, last, lastlog, syslog, event viewer, etc
- Generic Forensics investigation
 - TCT, TCTUtil, IRCR, WinHex, EnCase
- Searching tools

Eventlog



NtLast



```
E:\WINNT\System32\cmd.exe
D:\security\forensics\logreview>ntlast -f -r -v
Record Number: 764
ComputerName: TRISTAN
EventID: 529 - Failed Logon Attempt
Time Attempted: - Sat Jun 09 11:29:57am 2001
Details -
    ClientName: administrator
    ClientMachine: \\EGZ071
    ClientDomain: EGZ071
    LogonType: Remote

Record Number: 762
ComputerName: TRISTAN
EventID: 529 - Failed Logon Attempt
Time Attempted: - Sat Jun 09 11:29:57am 2001
Details -
    ClientName: administrator
    ClientMachine: \\EGZ071
    ClientDomain: EGZ071
    LogonType: Remote

Record Number: 516
ComputerName: TRISTAN
EventID: 529 - Failed Logon Attempt
Time Attempted: - Sat May 19 04:56:36pm 2001
```

DumpSec – Registry Permission

The screenshot shows the Somarsoft DumpAcl application window. The title bar reads "Somarsoft DumpAcl - \\geiersberg". The menu bar includes "File", "Edit", "Search", "Report", "View", and "Help". The main window displays a table of registry permissions. The table has four columns: "Path (exception keys)", "Account", "Own Key", and "Inheritable". The data is organized into groups of three rows each, corresponding to the registry path "HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes". Each group lists permissions for "SYSTEM", "Everyone", and "geiersberg\Administrators". The "Own Key" column shows "0" for SYSTEM and "all" for the other two accounts. The "Inheritable" column shows "all" for all accounts. The status bar at the bottom indicates "Processed 55849 registry keys" and "00019".

Path (exception keys)	Account	Own Key	Inheritable
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	SYSTEM	0	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	Everyone	read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	geiersberg\Administrators	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	SYSTEM	0	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	Everyone	read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	geiersberg\Administrators	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	SYSTEM	0	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	Everyone	read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	geiersberg\Administrators	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	SYSTEM	0	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	Everyone	read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	geiersberg\Administrators	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	SYSTEM	0	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	Everyone	read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	geiersberg\Administrators	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	SYSTEM	0	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	Everyone	read(QENR)	read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	geiersberg\Administrators	all	all
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Classes	SYSTEM	0	all

File Access - sfile

```
Copyright 2001 Forix Business Solutions.
Start search,987924423,Sun Apr 22 15:27:03 2001
File,Size,Last Access,Last Modification,Creation
e:\temp\Tin_Schultz.doc,72192,Mon Apr 16 00:00:00 2001,Tue Mar 13 07:38:34 2001,
Tue Mar 13 07:38:33 2001
e:\temp\tempdoc\cs425F.doc,33280,Sun Mar 18 00:00:00 2001,Fri Dec 17 19:14:34 19
99,Fri Dec 17 19:14:28 1999
e:\temp\tempdoc\adding.doc,24381,Fri Dec 15 00:00:00 2000,Tue Oct 26 07:29:44 19
99,Tue Oct 26 07:29:43 1999
e:\temp\tempdoc\reined.doc,40448,Sun Mar 18 00:00:00 2001,Thu Dec 3 22:36:00
1998,Thu Dec 3 22:35:58 1998
e:\temp\tempdoc\ntkern.doc,24381,Sun Mar 18 00:00:00 2001,Thu Oct 28 07:56:44 19
99,Thu Oct 28 07:56:42 1999
e:\temp\tempdoc\brutal97.doc,56320,Fri Dec 15 00:00:00 2000,Sat Jul 1 01:10:54
2000,Sat Jul 1 01:10:13 2000
e:\temp\tempdoc\act_sync.doc,497152,Mon Dec 25 00:00:00 2000,Fri Feb 19 14:03:20
1999,Fri Feb 19 14:00:19 1999
e:\temp\tempdoc\distributed_metastasis.doc,89088,Fri Dec 15 00:00:00 2000,Mon Jan
3 12:45:46 2000,Mon Jan 3 12:45:30 2000
e:\temp\tempdoc\NET_document.doc,41472,Fri Dec 15 00:00:00 2000,Wed Dec 23 14:53
:54 1998,Wed Dec 23 14:53:51 1998
e:\temp\tempdoc\San's Stuff\CON98MM.doc,23040,Fri Dec 15 00:00:00 2000,Mon Dec 2
1 16:26:36 1998,Mon Dec 21 16:26:03 1998
e:\temp\tempdoc\San's Stuff\CON98SMM.doc,30720,Fri Dec 15 00:00:00 2000,Mon Dec
21 16:27:38 1998,Mon Dec 21 16:27:01 1998
e:\temp\tempdoc\San's Stuff\PC_HK98.doc,171008,Fri Dec 15 00:00:00 2000,Tue Jan
5 15:47:12 1999,Mon Dec 21 16:28:58 1998
e:\temp\tempdoc\San's Stuff\FaxCover.doc,25088,Fri Dec 15 00:00:00 2000,Mon Dec
21 16:32:04 1998,Mon Dec 21 16:31:29 1998
e:\temp\tempdoc\San's Stuff\HR_contacts.xls,16896,Fri Dec 15 00:00:00 2000,Tue J
an 5 16:22:04 1999,Mon Dec 21 16:33:28 1998
e:\temp\tempdoc\San's Stuff\LIR98F_M.doc,73216,Fri Dec 15 00:00:00 2000,Mon Dec
21 16:43:34 1998,Mon Dec 21 16:42:55 1998
e:\temp\tempdoc\San's Stuff\LIR98F_U.doc,22016,Fri Dec 15 00:00:00 2000,Mon Dec
21 16:44:06 1998,Mon Dec 21 16:43:50 1998
e:\temp\tempdoc\San's Stuff\LIR98H_M.doc,171520,Fri Dec 15 00:00:00 2000,Tue Jan
5 15:40:38 1999,Mon Dec 21 16:44:12 1998
e:\temp\tempdoc\San's Stuff\LIR98H_U.doc,23552,Fri Dec 15 00:00:00 2000,Mon Dec
21 16:46:54 1998,Mon Dec 21 16:46:30 1998
e:\temp\tempdoc\San's Stuff\RES988_S.doc,31232,Fri Dec 15 00:00:00 2000,Mon Dec
21 16:47:48 1998,Mon Dec 21 16:47:31 1998
e:\temp\tempdoc\San's Stuff\SanR_A4.doc,25088,Fri Dec 15 00:00:00 2000,Mon Dec 2
1 17:21:54 1998,Mon Dec 21 16:51:34 1998
e:\temp\tempdoc\San's Stuff\ucsdata.doc,60416,Fri Dec 15 00:00:00 2000,Mon Dec 2
1 17:00:12 1998,Mon Dec 21 16:59:34 1998
e:\temp\tempdoc\San's Stuff\yaleclub.xls,150672,Fri Dec 15 00:00:00 2000,Mon Dec
21 17:02:38 1998,Mon Dec 21 17:00:18 1998
e:\temp\tempdoc\San's Stuff\hk97data.doc,37376,Fri Dec 15 00:00:00 2000,Tue Dec
```

```
Usage: sfile
-d Direc
  (defa
-g Look
-m Look
-o Look
-s Look

By default,
NOTE: Beginn
for ea

Copyright 20
Start search
File,Size,La
d:\temp\PPC_
01,Mon Jan
d:\temp\Sele
01,Thu Jan
d:\temp\Agen
Thu Jan 4 0
d:\temp\Qand
16 2001,Thu
d:\temp\Tran
4 10:04:42
d:\temp\Qand
06:24 2001,T
Search compl
E:\security\
```

```

D:\WINNT\System32\cmd.exe
ess\listdlls.exe

ListDLLs U2.23 - DLL lister for Win9x/NT
Copyright (C) 1997-2000 Mark Russinovich
http://www.sysinternals.com

-----
System pid: 8
Command line: <no command line>
-----
smss.exe pid: 152
Command line: \SystemRoot\System32\smss.exe

Base      Size      Version      Path
0x48580000 0xe000    \SystemRoot\System32\smss.exe
0x77f80000 0x7a000  5.00.2195.1600 D:\WINNT\System32\ntdll.dll
0x68010000 0xf6000  5.00.2195.0001 D:\WINNT\System32\sfcfiles.dll

-----
csrss.exe pid: 180
Command line: D:\WINNT\system32\csrss.exe ObjectDirectory=\Windows SharedSection
=1024,3072,512 Windows=0n SubSystemType=Windows ServerDll=basesrv,1 ServerDll=wi
n32rv:UserServerDllInitialization,3 ServerDll=win32rv:ConServerDllInitialization,2
ProfileControl=Off MaxRequestThreads=16

Base      Size      Version      Path
0x5fff0000 0x4000    \??\D:\WINNT\system32\csrss.exe
0x77f80000 0x7a000  5.00.2195.1600 D:\WINNT\System32\ntdll.dll
0x5ff90000 0xc000    5.00.2137.0001 D:\WINNT\system32\CSRSSRV.dll
0x5ffa0000 0xc000    5.00.2191.0001 D:\WINNT\system32\basesrv.dll
0x5ffb0000 0x40000  5.00.2195.1600 D:\WINNT\system32\win32rv.dll
0x77e10000 0x64000  5.00.2195.1600 D:\WINNT\system32\USER32.DLL
0x77e80000 0xb5000  5.00.2195.1600 D:\WINNT\system32\KERNEL32.DLL
0x77f40000 0x3c000  5.00.2195.1340 D:\WINNT\system32\GDI32.DLL

-----
winlogon.exe pid: 176
Command line: winlogon.exe

Base      Size      Version      Path
0x01000000 0x2d000  \??\D:\WINNT\system32\winlogon.exe
0x77f80000 0x7a000  5.00.2195.1600 D:\WINNT\System32\ntdll.dll
0x78000000 0x46000  6.01.8637.0000 D:\WINNT\system32\MSUCRT.DLL
0x77e80000 0xb5000  5.00.2195.1600 D:\WINNT\system32\KERNEL32.dll
0x77db0000 0x5a000  5.00.2195.1600 D:\WINNT\system32\ADVAPI32.DLL
0x77d40000 0x70000  5.00.2195.1615 D:\WINNT\system32\RPCRT4.DLL
0x77f40000 0x3c000  5.00.2195.1340 D:\WINNT\system32\GDI32.DLL
0x77e10000 0x64000  5.00.2195.1600 D:\WINNT\system32\USER32.DLL
0x77c10000 0x5d000  5.00.2195.1600 D:\WINNT\system32\USERENV.DLL
0x769a0000 0x7000  5.00.2137.0001 D:\WINNT\system32\NDDDEAPI.DLL
0x76980000 0x1b000  5.00.2195.1618 D:\WINNT\system32\SFC.DLL
0x68010000 0xf6000  5.00.2195.0001 D:\WINNT\system32\sfcfiles.dll
0x77be0000 0xf000  5.00.2195.1600 D:\WINNT\system32\SECUR32.DLL
0x690f0000 0xb000  5.00.2181.0001 D:\WINNT\system32\PROFMAP.DLL
0x75170000 0x4f000  5.00.2195.1600 D:\WINNT\system32\NETAPI32.dll
0x751c0000 0x6000  5.00.2134.0001 D:\WINNT\system32\NETRPF.DLL
0x75150000 0xf000  5.00.2160.0001 D:\WINNT\system32\SAMLIB.DLL
0x75030000 0x14000  5.00.2195.1340 D:\WINNT\system32\MS2_32.DLL
0x75020000 0x8000  5.00.2134.0001 D:\WINNT\system32\MS2HELP.DLL
0x77950000 0x29000  5.00.2195.1175 D:\WINNT\system32\WLDAP32.DLL

```

Handlex

The screenshot shows the Handlex application window with the following data:

Process	PID	Description	Owner	Priority	Handles	Window...
Exploer.exe	1908	Windows Explorer	\GEGERSBERG\vicci	8	407	strace
RealPlay.exe	1016	RealPlayer	\GEGERSBERG\vicci	8	165	
TsAdBot.exe	1008	TsAdBot	\GEGERSBERG\vicci	8	101	
msmsgs.exe	2056	MSN Messenger Service	\GEGERSBERG\vicci	8	138	
hpddr.exe	720	HP Lateset 1100 Document...	\GEGERSBERG\vicci	8	135	
AcroTray.exe	1384		\GEGERSBERG\vicci	8	20	
PGPTray.exe	1376	PGP System Tray Application	\GEGERSBERG\vicci	8	128	
msoffice.exe	1712	Microsoft Office 2000 compo...	\GEGERSBERG\vicci	8	69	
EnterNetFolder	1728		\NT AUTHORITY\SYSTEM	8	118	Profiles - ...
explore.exe	1224	Internet Explorer	\GEGERSBERG\vicci	8	608	Strace for...
ICQ.exe	1760	ICQ Application	\GEGERSBERG\vicci	8	154	
cmd.exe	2140	Windows NT Command Proc...	\GEGERSBERG\vicci	8	23	D:\WINN...
ntvdm.exe	2256	NTVDM.EXE	\GEGERSBERG\vicci	8	37	
WINWORD...	1788		\GEGERSBERG\vicci	8	209	Forensics...
Agent5vr.exe	2472	Microsoft Agent Server	\GEGERSBERG\vicci	8	84	
HandleEx.exe	2420	Handle and DLL Viewer	\GEGERSBERG\vicci	8	71	HandleEx...
ping.exe	1684	TCP/IP Ping Command	\GEGERSBERG\vicci	8	24	
ping.exe	2252	TCP/IP Ping Command	\GEGERSBERG\vicci	8	24	

Handle	Type	Access	Name
14	Directory	00000003	\KnownDlls
18	File	00100020	E:\security\forensics\Process\strace\strace\app\Debug
20	Directory	000F000F	\Windows
28	Mutant	00000001	\WinCacheMutant
38	WindowStation	000F037F	\Windows\WindowStations\WinSta0
3C	WindowStation	000F037F	\Windows\WindowStations\WinSta0
40	Desktop	000F01FF	\Default
44	Key	000F003F	HKLM
4C	Thread	001F03FF	ping.exe(2252): 2116
54	Key	000F003F	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
60	File	001200A0	\Device\Np
64	Key	000F003F	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5

ping.exe pid: 2252

```

D:\WINNT\System32\cmd.exe
RealPlay.exe pid: 1816 <GEIERSBERG:ricci>
 18: File D:\
 88: Section \BaseNamedObjects\smGlobalPnpInfo
 8c: Section \BaseNamedObjects\WDMAUD_Path_Size
 90: Section \BaseNamedObjects\WDMAUD_Path_Size
 94: Section \BaseNamedObjects\WDMAUD_Path_Size
 98: Section \BaseNamedObjects\WDMAUD_Path_Size
 9c: Section \BaseNamedObjects\WDMAUD_Path_Size
 a0: Section \BaseNamedObjects\WDMAUD_Path_Size
 a4: Section \BaseNamedObjects\WDMAUD_Path_Size
 a8: Section \BaseNamedObjects\WDMAUD_Path_Size
 b0: Section \BaseNamedObjects\WDMAUD_Path_Size
 b8: Section \BaseNamedObjects\WDMAUD_Callbacks
100: File D:\Program Files\Common Files\Real\Plugins\ExtResources\c
ore3260.xrs
228: Section \BaseNamedObjects\__R_0000000000cc_SMen__

-----
TsAdBot.exe pid: 1008 <GEIERSBERG:ricci>
 18: File D:\
168: Section \BaseNamedObjects\__R_0000000000cc_SMen__

-----
nsmgs.exe pid: 2056 <GEIERSBERG:ricci>
 18: File D:\
 68: Section \BaseNamedObjects\MessengerTeURL
  f8: Section \BaseNamedObjects\__R_0000000000cc_SMen__
10c: File D:\Program Files\Messenger\nsmgs.exe
114: File D:\WINNT\system32\stdole32.tlb
120: Section \BaseNamedObjects\smGlobalPnpInfo
124: Section \BaseNamedObjects\WDMAUD_Path_Size
128: Section \BaseNamedObjects\WDMAUD_Path_Size
12c: Section \BaseNamedObjects\WDMAUD_Path_Size
130: Section \BaseNamedObjects\WDMAUD_Path_Size
134: Section \BaseNamedObjects\WDMAUD_Path_Size
138: Section \BaseNamedObjects\WDMAUD_Path_Size
13c: Section \BaseNamedObjects\WDMAUD_Path_Size
140: Section \BaseNamedObjects\WDMAUD_Path_Size
148: Section \BaseNamedObjects\WDMAUD_Path_Size
150: Section \BaseNamedObjects\WDMAUD_Callbacks
238: File D:\Documents and Settings\ricci\Local Settings\Temporary
Internet Files\Content.IE5\index.dat
244: Section \BaseNamedObjects\D:\Documents and Settings\ricci\Local S
ettings_Temporary Internet Files_Content.IE5_index.dat_786432
24c: File D:\Documents and Settings\ricci\Cookies\index.dat
254: File D:\Documents and Settings\ricci\Local Settings\History\Hi
story.IE5\index.dat
258: Section \BaseNamedObjects\D:\Documents and Settings\ricci\Local S
ettings_History_History.IE5_index.dat_1835008
264: Section \BaseNamedObjects\D:\Documents and Settings\ricci\Cookies
_index.dat_98304

-----
hppddir.exe pid: 728 <GEIERSBERG:ricci>
 18: File D:\HPDESK
 68: File D:\HPDESK\TMAPPLNK.DBF
 6c: File D:\HPDESK\TMAPPLNK.CDX
 84: Section \BaseNamedObjects\HPPIELLO
 98: Section \BaseNamedObjects\H_SHARED
 ac: Section \BaseNamedObjects\HPPMLC00_MLGlobal_
 d4: Section \BaseNamedObjects\HPPML00PML_SHARED_MEM

```

Fport

```
D:\WINNT\System32\cmd.exe
pv: No matching processes found

E:\security\forensics\Process\strace\strace\app\Debug>E:\security\forensics\port
chk\fport.exe
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid      Process          Port  Proto Path
412      svchost          -> 135  TCP  D:\WINNT\system32\svchost.exe
8        System           -> 139  TCP
8        System           -> 445  TCP
576      MSTask           -> 1025 TCP  D:\WINNT\system32\MSTask.exe
8        System           -> 1027 TCP

412      svchost          -> 135  UDP  D:\WINNT\system32\svchost.exe
8        System           -> 137  UDP
8        System           -> 138  UDP
8        System           -> 445  UDP
228      services        -> 1026 UDP  D:\WINNT\system32\services.exe
1224    IEXPLORE        -> 1974 UDP  D:\Program Files\Internet Explorer\IEXPLORE
.EXE
648      PGPservice       -> 10000 UDP  c:\Program Files\Network Associates\PGP for
Windows 2000\PGPservice.exe

E:\security\forensics\Process\strace\strace\app\Debug>
```

PortMon

The screenshot shows the Portmon application window titled "Portmon on \\DUAL (local)". The window has a menu bar with "File", "Edit", "Capture", "Options", "Computer", and "Help". Below the menu bar is a toolbar with various icons. The main area contains a table with the following columns: "#", "Time", "Process", "Request", "Port", "Result", and "Other". The table lists 23 entries (rows 423 to 445) showing I/O requests from the process "tapisrv.exe" to the port "Serial0". The requests are a mix of "IRP_MJ_WRITE", "IOCTL_SERIAL_WAIT_ON_MASK", and "IRP_MJ_READ". All results are "SUCCESS". The "Other" column contains hex dump-like data for each request.

#	Time	Process	Request	Port	Result	Other
423	4:44:23 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ~...IE..<^.....P.....
424	4:44:23 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
425	4:44:23 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 8: ~...IE..
426	4:44:23 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
427	4:44:23 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 60: <.o.>.@9.P.....Q\...
428	4:44:23 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 72: ~...IE..@+.....h.....
429	4:44:23 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
430	4:44:23 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 8: ~...IE..
431	4:44:23 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
432	4:44:23 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 209: ..p.>?...P.....5.....
433	4:44:23 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ~...IE..<.....^.....
434	4:44:24 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ~...IE..<.....^.....
435	4:44:25 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ~...IE..<.....^.....
436	4:44:26 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 71: ~...IE..?/?.....d.....P.....
437	4:44:26 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
438	4:44:26 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 8: ~...IE..
439	4:44:26 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
440	4:44:26 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 469: ..q.>...>...P.....5.....
441	4:44:26 PM	tapisrv.exe	IRP_MJ_WRITE	Serial0	SUCCESS	Length 68: ~...IE..<0...Z.....
442	4:44:26 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
443	4:44:26 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 8: ~...IE..
444	4:44:26 PM	tapisrv.exe	IOCTL_SERIAL_WAIT_ON_MASK	Serial0	SUCCESS	
445	4:44:26 PM	tapisrv.exe	IRP_MJ_READ	Serial0	SUCCESS	Length 60: <y..5.....M\.....

Network status check

```
E:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

E:\>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP   tristan:1043           205.188.8.69:telnet    ESTABLISHED
TCP   tristan:1110           www.technotronic.com:ftp  CLOSE_WAIT
TCP   tristan:1112           www.technotronic.com:28699  CLOSE_WAIT
TCP   tristan:1136           206.97.79.222:http      CLOSE_WAIT
TCP   tristan:1151           206.97.79.222:http      CLOSE_WAIT
TCP   tristan:1155           206.97.79.222:http      CLOSE_WAIT
TCP   tristan:1157           206.97.79.222:http      CLOSE_WAIT
TCP   tristan:1221           206.97.79.222:http      CLOSE_WAIT
TCP   tristan:1222           206.97.79.222:http      CLOSE_WAIT
TCP   tristan:1223           206.97.79.222:http      CLOSE_WAIT
TCP   tristan:1308           shekkipmei.pacific.net.hk:pop3  TIME_WAIT

E:\>_
```

Step 3 - Investigation

- Identify the “first handle” of the case
- Obtain volatile data
- Review logs, system setting files
- Determine the possible source of evidence
 - Network connection in router, firewall
 - Sniffer and IDS packet captured
 - System, Web and FTP log files
 - Trace of CPU usage, process running on the machine
 - Possible hidden files, deleted files and updated files
 - Open ports, services, files
 - Email message header
 - Possible installation of root kits

Step 3 - Further Investigation

Further Investigation

- Check where is the attack from
- Determine the suspected process using ps, lsof
- Capturing process memory using core dump (in Unix, gcore PID)
- Capture Process information
- Examine the core using strings
- Determine backdoor
- Watching process action
- Undelete files
- Search the slack space
- Review pagefiles.sys, Recycle Bin, Printer spool
- Search hidden information in picture and document

File handling tools - sig

```
D:\WINNT\System32\cmd.exe

E:\security\forensics\FileTrace>ren 08.pdf 08.gif

E:\security\forensics\FileTrace>sig 08.gif
Signature file successfully read.
File: 08.gif
Ext : gif
Hex : 255044462D312E330D25E2E3CFD30D0A31302030

File signature does not match extension.

E:\security\forensics\FileTrace>sig /?
Signature file successfully read.
File: /?
Ext : none
Could not open /?: Invalid argument

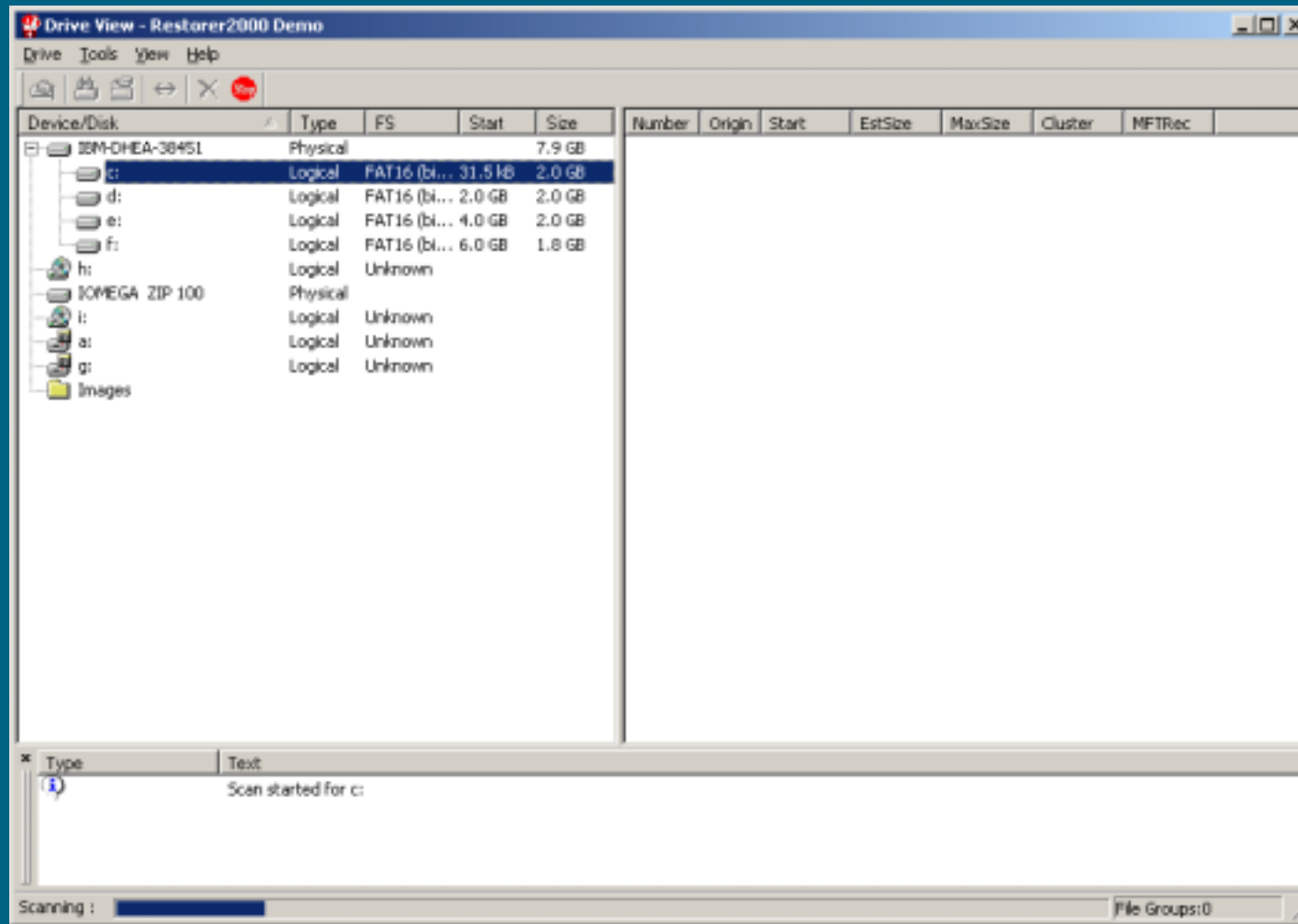
E:\security\forensics\FileTrace>ren 08.gif 08.pdf

E:\security\forensics\FileTrace>sig 08.pdf
Signature file successfully read.
File: 08.pdf
Ext : pdf
Hex : 255044462D312E330D25E2E3CFD30D0A31302030

File extension corresponds to file signature.

E:\security\forensics\FileTrace>
```

Undelete



WinHex

The screenshot shows the WinHex application window titled "WinHex - [Kernel32.dll]". The main window is a hex editor displaying the contents of the file "Kernel32.dll" located at "C:\WIN98\SYSTEM". The hex editor shows a list of offsets from 0005A000 to 0005A1D0. A "Data Interpreter" dialog box is open, displaying various data types and their values for the selected hex data. The dialog box includes a list of data types on the left and their corresponding values on the right. The values include: 8 Bit (±): 80, 8 Bit (+): 80, 16 Bit (±): -14256, 16 Bit (+): 51280, 32 Bit (±): 17352784, 32 Bit (+): 17352784, 64 Bit (±): 678354693890033744, Binary: 01010000, Float: 2.512297e-38, Real: 1.7763570584e-15, Double: 2.58028187477518e-2, Long Dbl: NAN, ASM: PUSH, DOS Date: 08/09/1980, FILETIME: 01:02:32, FILETIME: 08/15/3750, OLE Date: 12/30/1989, ANSI SQL: 03/09/49369, UNIX Date: 04:23:14, and UNIX Date: 07/20/1970. The status bar at the bottom shows "Page 769 of 999", "Offset: 5A000", and "= 108".

Data Type	Value
8 Bit (±)	80
8 Bit (+)	80
16 Bit (±)	-14256
16 Bit (+)	51280
32 Bit (±)	17352784
32 Bit (+)	17352784
64 Bit (±)	678354693890033744
Binary	01010000
Float	2.512297e-38
Real	1.7763570584e-15
Double	2.58028187477518e-2
Long Dbl	NAN
ASM	PUSH
DOS Date	08/09/1980
FILETIME	01:02:32
FILETIME	08/15/3750
OLE Date	12/30/1989
ANSI SQL	03/09/49369
UNIX Date	04:23:14
UNIX Date	07/20/1970

Investigation of victim machine

C:\WINNT\System32\cmd.exe

CSRSS	24	13	8	272	736	0:00:04.546	0:00:20.118	2:52:06.08
WINLOGON	35	13	4	83	2364	0:00:00.230	0:00:03.204	2:52:02.77
SERVICES	41	9	21	256	3276	0:00:00.440	0:00:05.467	2:51:59.25
LSASS	44	9	13	107	2724	0:00:00.260	0:00:01.672	2:51:58.19
SPOOLSS	73	8	6	56	612	0:00:00.090	0:00:00.350	2:51:39.03
RPCSS	94	8	8	122	1012	0:00:00.100	0:00:00.380	2:50:51.17
NDDEAGNT	101	8	1	16	580	0:00:00.010	0:00:00.070	2:50:49.28
msdtc	106	8	16	104	3128	0:00:00.280	0:00:02.623	2:50:46.13
llssrv	127	9	9	69	804	0:00:00.010	0:00:00.220	2:50:41.39
PSTORES	136	8	5	47	852	0:00:00.070	0:00:00.600	2:50:41.11
LOCATOR	144	8	5	37	580	0:00:00.080	0:00:00.050	2:50:40.82
mstask	154	8	6	76	924	0:00:00.060	0:00:00.380	2:50:40.35
inetinfo	147	8	28	409	11116	0:00:20.319	0:00:05.317	2:50:39.55
EXPLORER	169	8	11	86	1760	0:00:01.402	0:00:14.290	2:50:38.74
LOADWC	192	8	2	24	580	0:00:00.060	0:00:00.090	2:50:32.53
UMTBox	196	8	2	23	1124	0:00:02.313	0:00:00.280	2:50:32.30
CMD	199	8	1	22	704	0:00:00.480	0:00:02.503	2:50:13.88
CMD	223	8	1	20	48	0:00:00.010	0:00:00.040	0:53:21.22
CMD	217	8	1	20	420	0:00:00.030	0:00:00.070	0:50:38.44
CMD	221	8	1	186	1260	0:00:00.040	0:00:00.220	0:50:36.97
pslist	210	8	1	46	1896	0:00:00.040	0:00:00.260	0:00:01.41
more.com	208	8	1	14	1196	0:00:00.020	0:00:00.010	0:00:01.35

F:\forensics\Process\pstools>

1 object(s) selected 1.06MB

The virtual machine is running.

Investigation of log files

Step 4 - Summarize and Presentation

- Summarize the cause and source of the incident
- Construct the chronological map of the events
- Presentation of the investigation procedures and findings
- Determine the explanations of the case

Sample Logs from real case

```
sp 404;http://10.2.1.2/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%c1%af../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 69 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 72 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 75 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 78 80 HTTP/1.0 - -  
sp 404;http://10.2.1.2/msadc/..%e0%80%af../..%e0%80%af../..%e0%80%af../winnt/system32/cmd.exe?/
```

Microsoft Word - hp17

Daily Log Review Report

HP Service Incident Response Team		Case No:	Log Review No: [REDACTED]
First Name: [REDACTED]	Last Name: [REDACTED]	Chinese Name:	
Contact phone: [REDACTED]	Mobile:	Email: [REDACTED]	
Position: Security Consultant		Department: HP e-Security Center	

Log

<p>Log file name:</p> <p>[REDACTED]</p> <p><u>Server1_eventlog.zip</u></p> <p><u>Exchange_eventlog.zip</u></p> <p><u>17May2001_cpfwlog.zip</u></p> <p><u>Firewall_eventlog.zip</u></p> <p><u>17May_isslog.zip</u></p>	<p>Collected from:</p> <p>web servers 1</p> <p>firewall-1</p> <p>exchange server</p> <p><u>RealSecure</u></p>	<p>Purpose:</p> <p>web server log</p> <p>exchange server and</p> <p>firewall-1 log</p> <p>IDS log</p>
<p>Summary of the log file</p>	<p>An attack originated from [REDACTED] attempting to attack the vulnerability as stated in "MS00-086 : Web Server File Request Parsing Vulnerability" http://www.microsoft.com/technet/security/bulletin/MS00-086.asp</p> <p>The attack was not successful and the attacker was returned with the error page <u>"/secure/under_construct.asp"</u></p>	

Page 1 Sec 1 1/2 At 2.1" Ln 3 Col 1 REC TRK EXT OVR WPH [REDACTED]

Conclusion

- Vulnerabilities and bugs are always with you
- No security vendors can eliminate them all
- Incident Handling and Forensics Investigation Service is one of the key Solutions in Security Risk Management
- Everyone can participate in Cyber-Investigation
- Early identification and containment of cyber-crime is helpful to the Cyber Crime Investigation

Thank you.

HP e-Security Center

- Tel: 25997126

Ricci Ieong

- Tel: 25994717
Fax: 25069259
email: ricci-sc_ieong@hp.com

Vincent Ip

- Tel: 25994224
Fax: 25069259
email: vincent-tp_ip@hp.com